PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-174443
(43)Date of publication of application : 20.06.2003

(51)Int.Cl. H04L 9/08
G06F 15/00
G06F 17/60
H04L 9/32

(21)Application number : 2001-373674 (71)Applicant : SONY CORP
(22)Date of filing : 07.12.2001 (72)Inventor : ISHII HIDEHIRO

(54) INFORMATION PROCESSOR AND INFORMATION PROCESSING METHODPROGRAM STORAGE MEDIUMAND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To freely deliver and distribute contentsand to flexibly set a license for using the contents.
SOLUTION: A contents server encrypts contents in providing the contents via the Internet to a client. Thenattribute information associated with the contents is described in the header of the encrypted contents. The client acquires a license to permit the encrypted contents by performing an access to a license server to acquire a license where the attribute information of the contents fulfills an attribute condition.

CLAIMS

[Claim(s)]
[Claim 1]A content reception means to receive contents including enciphered content data and attribution informationA license reception means which receives a license including a content storing means which memorizes said contentsand an attribute condition which indicated conditions about said attribution information of contents which can be usedA license memory measure which memorizes said licenseand a judging means a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding means which decodes said enciphered content data of said contents based on said judging means having judged with said attribution

information of said contents fulfilling an attribute condition of the license concernedAn information processor provided with an output means which outputs contents data decoded by said decoding means.
[Claim 2]The information processor according to claim 1 characterized by what said contents contain a contents key for decoding said contents data further for.
[Claim 3]The information processor according to claim 1 characterized by what said attribution information consists of combination of an attribute item and an attribute value.
[Claim 4]The information processor according to claim 1 characterized by what said attribute item is prescribed for by information about a record companyan artista release daya contents publishera genresubscriptionor a label.
[Claim 5]The information processor according to claim 1 characterized by what said attribute condition consists of an attribute iteman attribute valueand combination of a operator.
[Claim 6]A reception means which receives a license request containing license ID which identifies uniquely a license including an attribute condition which indicated conditions about attribution information included in contentsA memory measure which memorizes a license with license IDand an incorporation means to incorporate said license corresponding to said license ID contained in said license requestAn information processor provided with a signature means which adds an electronic signature to said licenseand a transmitting means which transmits a license signed by a signature means.
[Claim 7]The information processor according to claim 6 provided with a license processing means to add terminal ID to a license incorporated by said incorporation means.
[Claim 8]A memory measure which memorizes contents including enciphered content data and attribution informationA reception means which receives a contents request containing content ID which identifies contents uniquelyAre an information processor provided with a transmitting means which transmits contents corresponding to content ID contained in a contents requestand said attribution information included in said contentsIt is the information used in order to judge whether an attribute condition of a license is fulfilledwhen using the contents concerned.
An information processor characterized by what an attribute condition of said license is the information which indicated conditions about said attribution information of said contents which can be used.

[Claim 9]A content reception step which receives contents including enciphered content data and attribution informationA license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used to be the contents memory steps which memorize said contentsA license memory step which memorizes said

licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedAn information processing method containing an output step which outputs contents data decoded by said decoding means.
[Claim 10]A content reception step which receives contents including enciphered content data and attribution informationA license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used to be the contents memory steps which memorize said contentsA license memory step which memorizes said licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedA program which makes a computer perform an output step which outputs contents data decoded by said decoding means.
[Claim 11]A content reception step which receives contents including enciphered content data and attribution informationA license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used to be the contents memory steps which memorize said contentsA license memory step which memorizes said licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedA program storing medium with which a program which makes a computer perform an output step which outputs contents data decoded by said decoding means was stored.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about an information processor and a methoda program storing mediumand a programThe contents which have not been licensed in particular from an owner of a copyright are copied unjustlyand are related with the

information processor and method and program storing medium which enabled it to prevent being usedand a program.
[0002]
[Description of the Prior Art]These daysas a user provides other users with the music data which he holds via the Internet and offers are received for the music data which he does not hold from other usersthe system where two or more users exchange music data for nothing and which they suit is realized.
[0003]If the contents of one music and others exist theoreticallyin order that other users of all the may be enabled to use it and many users may not purchase contents in such a systemSince the owner of a copyright about contents cannot sell the contents as workshe will lose an opportunity to receive the loyalty about use of the works which can originally be received with sale of works.
[0004]Thenthe contents distributed are encipheredand if the license for using the contents is published separately and it does not have the license corresponding to the enciphered contentsthere is a system decodes contents and made it prevent from reproducing.
[0005]The copyright of works can be protected making it possible to distribute contents freely by doing in this way.
[0006]
[Problem(s) to be Solved by the Invention]howeverthe license which set the correspondence relation of contents to the license flexiblyor was already distributed in the above-mentioned system -- it was difficult to newly distribute the contents which can be used.
[0007]This invention is made in view of such a situationcontents are distributed and circulated freelyand it enables it to set up freely a set of the contents which can be used according to a license.
[0008]
[Means for Solving the Problem]This invention is characterized by the 1st information processor comprising the following.
A content reception means to receive contents including enciphered content data and attribution information.
A content storing means which memorizes said contents.
A license reception means which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used.
A license memory measure which memorizes said licenseand a judging means a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding means in which said judging means decodes said enciphered content data of said contents based on having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedand an output means

which outputs contents data in which it was decoded by said decoding means.

[0009]Said contents can contain a contents key for decoding said contents data further.
[0010]Said attribution information can consist of combination of an attribute item and an attribute value.
[0011]Information about a record companyan artista release daya contents publishera genresubscriptionor a label can prescribe said attribute item.
[0012]Said attribute condition can consist of an attribute iteman attribute valueand combination of a operator.
[0013]This invention is characterized by the 2nd information processor comprising the following.
A reception means which receives a license request containing license ID which identifies uniquely a license including an attribute condition which indicated conditions about attribution information included in contents.
A memory measure which memorizes a license with license ID.
An incorporation means to incorporate said license corresponding to said license ID contained in said license request.
A signature means which adds an electronic signature to said licenseand a transmitting means which transmits a license signed by a signature means.

[0014]It can have a license processing means to add terminal ID to a license incorporated by said incorporation means.
[0015]A memory measure which memorizes contents in which the 3rd information processor of this invention includes enciphered content data and attribution informationA reception means which receives a contents request containing content ID which identifies contents uniquelyAre an information processor provided with a transmitting means which transmits contents corresponding to content ID contained in a contents requestand said attribution information included in said contentsIt is characterized by being the information used in order to judge whether an attribute condition of a license is fulfilledwhen using the contents concernedand an attribute condition of said license being the information which indicated conditions about said attribution information of said contents which can be used.
[0016]This invention is characterized by an information processing method comprising the following.
A content reception step which receives contents including enciphered content data and attribution information.
A contents memory step which memorizes said contents.
A license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used.

A license memory step which memorizes said licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedand an output step which outputs contents data decoded by said decoding means.

[0017]A content reception step which receives contents in which a program of this invention includes enciphered content data and attribution informationA license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used to be the contents memory steps which memorize said contentsA license memory step which memorizes said licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedIt is a program which makes a computer perform an output step which outputs contents data decoded by said decoding means.
[0018]A program stored in a program storing medium of this inventionA content reception step which receives contents including enciphered content data and attribution informationA license receiving step which receives a license including an attribute condition which indicated conditions about said attribution information of contents which can be used to be the contents memory steps which memorize said contentsA license memory step which memorizes said licenseand a determination step a license memorized by said license storage parts store judges whether said attribution information of said contents fulfills an attribute condition of the license concerned to beA decoding step which decodes said enciphered content data of said contents based on said judging means having judged with said attribution information of said contents fulfilling an attribute condition of the license concernedIt is a program which makes a computer perform an output step which outputs contents data decoded by said decoding means.
[0019]
[Embodiment of the Invention]Drawing 1 shows the composition of the contents providing system which applied this invention. Client 1-11-2 (hereafterwhen these clients do not need to be distinguished separatelythe client 1 is only called) is connected to the Internet 2. In this examplealthough two clients are shownthe client of the arbitrary number is connected to the Internet 2.
[0020]On the Internet 2. When the contents server 3 which provides contents to the client 1the license server 4 which gives a license required to use the contents which

the contents server 3 provides to the client 1and the client 1 receive a licenseThe fee collection server 5 which performs accounting to the client 1 is connected.
[0021]These contents servers 3the license server 4and the fee collection server 5 are also connected to the arbitrary number and the Internet 2.
[0022]Drawing 2 expresses the composition of the client 1.
[0023]In drawing 2CPU(Central Processing Unit) 21Various kinds of processings are performed according to the program memorized by ROM(Read Only Memory) 22 or the program loaded to RAM(Random Access Memory) 23 from the storage parts store 28. the timer 20 -- a time check -- it operates and time information is supplied to CPU21. To RAM23CPU21 performs various kinds of processings againand also required data etc. are memorized suitably.
[0024]The encryption decoding part 24 performs processing which decodes the already enciphered contents data while enciphering contents data. The codec part 25 encodes contents data by ATRAC(Adaptive Transform Acoustic Coding)3 method etc.for exampleIt is made to supply and record on the semiconductor memory 44 connected to the drive 30 via the input/output interface 32. Or the codec part 25 decodes the data which was read from the semiconductor memory 44 via the drive 30 and which is encoded again.
[0025]The semiconductor memory 44 is constituted by the memory stick (trademark) etc.for example.
[0026]CPU21ROM22RAM23the encryption decoding part 24and the codec part 25 are mutually connected via the bus 31. The input/output interface 32 is also connected to this bus 31 again.
[0027]The input part 26CRT which become the input/output interface 32 from a keyboarda mouseetc.The communications department 29 which comprises the storage parts store 28a modema terminal adopteretc. which comprise the outputting part 27 which consists of a display which consists of LCD etc.a loudspeakeretc.a hard disketc. is connected. The communications department 29 performs the communications processing through the Internet 2. The communications department 29 performs the communications processing of an analog signal or a digital signal among other clients again.
[0028]The drive 30 is connected to the input/output interface 32 again if neededIt is suitably equipped with the magnetic disk 41the optical disc 42the magneto-optical disc 43or the semiconductor memory 44and the computer program read from them is installed in the storage parts store 28 if needed.
[0029]Although a graphic display is omittedthe contents server 3the license server 4and the fee collection server 5 are also constituted by the client 1 shown in drawing 2and the computer which has the same composition fundamentally.
[0030]Nextwith reference to the flow chart of drawing 3the client 1 explains the processing which receives offer of contents from the contents server 3.
[0031]When a user orders it access to the contents server 3 by operating the input

part 26CPU21 controls the communications department 29 and he makes it access the contents server 3 via the Internet 2. In Step S2a user operates the input part 26and if the contents which receive offer are specifiedCPU21 will receive this specification information and will notify the contents specified as the contents server 3 via the Internet 2 from the communications department 29. The contents server 3 which received this notice so that it may mention later with reference to the flow chart of drawing 4Since the enciphered contents data is transmittedin Step S3 CPU21If this contents data is received via the communications department 29that contents data enciphered will be supplied and stored in the hard disk which constitutes the storage parts store 28 in step S4.

[0032]Nextwith reference to the flow chart of drawing 4contents offer processing of the contents server 3 corresponding to the above processing of the client 1 is explained. In the following explanationthe composition of the client 1 of drawing 2 is quoted also as composition of the contents server 3.

[0033]In Step S21CPU21 of the contents server 3It stands by until it receives access from the Internet 2 from the client 1 via the communications department 29and when it judges with having received accessit progresses to Step S22 and the information which specifies the contents transmitted from the client 1 is incorporated. The information which specifies these contents is information which the client 1 has notified in Step S2 of drawing 3.

[0034]In Step S23CPU21 of the contents server 3 reads the contents specified for the information incorporated by processing of Step S22 out of the contents data memorized by the storage parts store 28. CPU21 supplies the contents data read from the storage parts store 28 to the encryption decoding part 24and makes it encipher in Step S24.

[0035]Since the contents data memorized by the storage parts store 28 is already encoded by the codec part 25 with ATRAC3 methodthis contents data encoded will be enciphered.

[0036]Of coursethe storage parts store 28 can be made to memorize contents data in the state where it enciphered beforehand. In this caseprocessing of Step S24 can be omitted.

[0037]Nextin Step S25CPU21 of the contents server 3 adds the attribution information which shows the variety of information about a key required to decode the contents enciphered and contents to the header which constitutes the format which transmits the enciphered contents data. And in Step S26 CPU21 of the contents server 3The data which formatted the contents enciphered by processing of Step S24 and the header which added a keyattribution informationand its electronic signature by processing of Step S25 is transmitted to the accessed client 1 via the Internet 2 from the communications department 29.

[0038]Drawing 5 is carried out in this wayand expresses the composition of the format in case contents are supplied to the client 1 from the contents server 3. This

format is constituted by header (Header) and the data (Data) as shown in the figure.
[0039]The electronic signature which signed the header with the encryption key of the license server in attribution information (Attribute List) and attribution informationThe contents key Kc (KR (Kc)) enciphered by the INEBU ring key block (EKB (Enabling KeyBlock)) and the route key KR obtained by carrying out decoding processing of the EKB using DNK is arranged.
[0040]Two or more entries of the attribute which consists of combination of an attribute item and an attribute value are described by attribution information.
[0041]The kind of attribute item is shown in drawing 6. CIDRCIDCIIDAIDGIDand LID are ID which identifies contentsa record companya contents publisheran artista genreand a label uniquelyrespectively. RelDate expresses the release day of contents. Subscription ID is an attribute item used for the subscription license mentioned later.
[0042]URL is address information accessed when acquiring the license for using contentsand is an address of the license server 4 specifically required in the case of the system of drawing 1since it is licensed.
[0043]Data is constituted by arbitrary numbers of encryption blocks (Encryption block). Each encryption block is constituted by an initial vector (IV (Initial Vector))the seed (Seed)and data EK'c (data) that enciphered contents data by key K'c.
[0044]Key K'c is constituted by the value which was adapted for the hash function and calculated the value Seed set to the contents key Kc by random numbers as shown in a following formula.
[0045]K'c=Hash(KcSeed)[0046]The initial vector IV and the seed Seed are set as a different value for every encryption block.
[0047]The data of contents is classified per 8 bytes and this encryption is performed every 8 bytes. 8 bytes of latter encryption is performed in the CBC (Cypher Block Chaning) mode performed using the result of 8 bytes of encryption of the preceding paragraph.
[0048]Since 8 bytes of encryption result of the preceding paragraph does not exist when enciphering 8 bytes of first contents data in the case of the CBC modewhen enciphering 8 bytes of first contents dataencryption is performed by making the initial vector IV into an initial value.
[0049]By performing encryption by this CBC modeeven if one encryption block is decodedit is controlled that that influence attains to other encryption blocks.
[0050]About this encryptiondrawing 14 and drawing 15 are made reference and explained in full detail behind.
[0051]The client 1 is no charge about the contents server 3 to contents as mentioned aboveand it can acquire freely.
[0052]Howevereach client 1 needs to acquire a licensewhen using the acquired contents.
[0053]When acquiring a licensethe client 1 performs registration processing to a license server on-line or off-line a prioriand acquires service information. A device

node key (DNK) and terminal ID are contained in service informationand it is used for carrying out decoding processing of the EKB. The license acquired from service information and a license server is saved at the storage parts store 28 of the client 1 secure one.

[0054]The composition of a license is shown in drawing 7. License IDa time stampthe expiration datean attribute conditiona use ruleand the electronic signature that signed these with the secret key of the license server are included in a license. A time stamp expresses the date of issue of a license. When the expiration date expresses the expiration date which can use a license and passes over this expiration dateit becomes impossible to use that license. An attribute condition expresses the conditions of the attribute of the contents which can use the client 1 which possesses the license by the conditional expression which consists of combination of the value about an attribute item and an attribute itema comparison operatorand a logical operator. The rule for using the contents which can use the license for a use rule is describedand the same terminal ID as what is contained in service information is contained.

[0055]The example of license composition realizable with combination with the attribution information included in contents below and the attribute condition included in a license is shown.

[0056]It is described as follows by the attribution information of the contents c1.

c1 : cid = {1} and aid = {01}reldate = November 102000 [0057]As for thiscontent ID expresses that 0 and 1 (namelycollaboration of the artist of No. 0 and the artist of No. 1)and the release day of 1 and artist ID are on November 102000.

[0058]Similarlyit is described as follows by the attribution information of the contents c2c3and c4.

c2 : cid = {2} and aid =. {0}December [reldate = 2000 year] 20 c3 : cid = {3} and aid = {0}March [reldate = 2001 year] 1 c4 : cid = {4} and aid = {0} and reldate = On October 212001 on the other handIt is described as follows by the attribute condition of the license l1.

l1 : cid ** 1 ** cid ** 2 [0059]Therebythe right of use r1 corresponds to the contents c1 and c2. That isthe contents c1 and c2 can be used in a terminal with the effective right of use r1.

[0060]The attribute condition of the license l2 is described as follows.

l2 : aid ** 0 ** (January 12001 < reldate < December 312001) [0061]This is the conditions of the meaning of the contents of the artist of No. 0 released in 2001and the license l2 corresponds to the contents c3 and c4. At this timethe contents c3 and c4 can be used at a terminal with the effective license l2. Suppose that the contents c5 which gave the following attribution information behind were published.

c5 : cid = {5} and aid = {0} and reldate = {December 12001} [0062]If these contents download and come to hand from the contents server 3it is not necessary to newly connect with a license server etc.and the contents c5 can also be used in the client 1

which has already held the license l2.
[0063]If a distribution entrepreneur is newly going to put on the market after distribution of these contents combining the contents c1c2and c5 as a best versionIf the following licenses l3 corresponding to it are publishedit is not necessary to newly create contentsthe contents under distributed – circulation are utilized as it isand the best version sale is possible.
l3 : cid ** 1 ** cid ** 2 ** cid ** 5 [0064]Thusa new issue can be easily made in the right of use which combined the contents under distributed – circulation. For examplethe Shinji Tanimura complete works in 1990 – 1999 can newly be put on the market by publishing the license with the attribute condition which restrained the release day and the artist.
[0065]The Morning Musume family complete works (what collected the contents of Morning MusumePUTCHIMONIYuuko Nakazawaand other related artists) can newly be put on the market by publishing the license with the attribute condition which restrained the artist.
[0066]The Alfee Best (for examplecontent ID is restrained).
[0067]Nextthe example which defines the license which comes to be able to carry out additional use of the newly released piece of music of some every month as subscription service is shown.
[0068]The conditions of the attribute of the license l4 are defined as follows.
l4 : cid ** 3 ** cid ** 4 ** sid ** 1 [0069]In the client 1 which possesses this license l4the contents c3 and c4 already published first are available. Suppose that the contents c6 and c7 which had the following attribution information as a newly released piece of music were published next month.
c6: cid = {6}sid = {1}c7: cid = {7}sid = {1} [0070]In this casethe client 1 with the license l4 does not newly need to purchase a licenseand can use the contents c6 and c7. The client 1 which has the license l4 by similarly publishing the contents which contained one in subscription ID every month can add available contentswithout purchasing a license separately.
[0071]Thusa set of the contents which can be used can be flexibly set up now by expressing an attribute condition with the combination of operatorssuch as an attribute iteman attribute value and a logical operatorand a relational operator.
[0072]the operator included in an attribute condition is mentioned here –– **** –– it is not limited but other various operators can be used.
[0073]With reference to drawing 8processing in case the client 1 reproduces contents is explained.
[0074]In Step S41CPU21 of the client 1 acquires the content ID to which it pointed because a user operates the input part 26.
[0075]And CPU21 reads the attribution information described by the header of contents data applicable if content ID is acquired.
[0076]Nextit is judged whether it progresses to Step S42and the license with which

the attribution information read at Step S41 fills the use contents conditional expression described by each license is already acquired by the client 1and CPU21 is memorized by the storage parts store 28. When such a license is not foundit progresses to Step S43 and CPU21 displays the message which urges acquisition of a license to a display via the outputting part 27.

[0077]In Step S42when judged with the license already being acquiredit progresses to Step S44 and it is judged whether the license from which CPU21 is acquired is a thing within the term of validity. it comes out to compare with the term specified as contents of the license and the present date clocked by the timer 20and it is judged whether a license is a thing within the term of validity. When judged with the term of validity of a license having already expiredit progresses to Step S45 and CPU21 performs a license update process. The details of this license update process are later mentioned with reference to the flow chart of drawing 8.

[0078]When judged with a license being still within the term of validity in Step S44Or in Step S45when a license is updatedit progresses to step S45' and CPU21 verifies the electronic signature included in the electronic signature included in the header of contentsand a license by the public key of the license server 4. When an electronic signature is judged to be the right as a result of verification of an electronic signatureit progresses to Step S46and CPU21 reads the contents data enciphered from the storage parts store 28and is made to store it in RAM23. And CPU21 is the encryption block unit arranged at the data of drawing 5and makes the encryption decoding part 24 supply and decode the data of the encryption block memorized by RAM23 in Step S47.

[0079]CPU21 supplies the contents data decoded by the encryption decoding part 24 to the codec part 25and makes it decode in Step S48 further. And from the input/output interface 32CPU21 supplies the data decoded by the codec part 25 to the outputting part 27carries out D/A conversionand makes it output from a loudspeaker.

[0080]A client explains the processing which carries out income of the license from the license server 4 using drawing 9 – drawing 11.

[0081]Drawing 9 shows license acquisition processing when the contents which the user of the client 1 wants to use are decided. When a user specifies contents by operating the input part 26 and directs the demand of a license list to the license server 4CPU21The communications department 29 is controlled and the license list request containing the content ID of the contents specified as the contents server 3 via the Internet 2 is transmitted. If a license list request is receivedthe license server 4 from the content ID contained in the received license list. The license list for which the list of the contents which extract an available license and can use applicable contents license ID of each licensethe conditions of the contents which can carry out a license name and useand nowthe service condition of contentsetc. were indicated is transmitted to the client 1.

[0082]If the client 1 receives a license list from the license server 4CPU21 will display the information on each license included in a license list at the outputting part 27. When the license for which a user asks with reference to the information is chosenCPU21After controlling the communications department 29 and forming a session by mutual recognitionsuch as SSLthe license request containing license ID of a license and terminal ID which were chosen as the contents server 3 via the Internet 2the user ID for fee collectionand a password is encipheredand it transmits. If the license server 4 is received [the license request transmitted from the client 1]after performing license issue processing mentioned laterit transmits the license corresponding to license ID contained in a license request to the client 1. If the license transmitted from the license server 4 is receivedthe client 1 carries out encryption etc. and saves the received license in the secure state at the storage parts store 28.

[0083]The user can acquire the license for using the contents which the client 1 has already possessed as mentioned above. The above license acquisition processing may be made to be started automaticallywhen it is operated and the license for reproducing the contents is not acquired [at which the contents which the user possesses in the client were reproduced].

[0084]Nexta user specifies various search conditions and shows drawing 16 the processing which searches and acquires a license. Firsta license name for a user to search a license neededIf search conditionssuch as the kind of licensea title of the contents which a license makes availablean album namea genrean artist nameand a release dayare specified by operating the input part 26CPU21 transmits the license list request containing the data which controlled the communications department and formatted the inputted search condition to the contents server 3. If the license list request transmitted from the client 1 is receiveda contents serverThe license by which the search condition included in a license list request is fulfilled is searched from the storage parts store 28and a license list including the information about each license of license ID etc. is transmitted to the client 1.

[0085]If the client 1 receives a license list from the license server 4CPU21 will display the information on each license included in a license list at the outputting part 27. When the license for which a user asks with reference to the information is chosenCPU21After controlling the communications department 29 and forming a session by mutual recognitionsuch as SSLthe license request containing license ID of a license and terminal ID which were chosen as the contents server 3 via the Internet 2the user ID for fee collectionand a password is encipheredand it transmits. If the license server 4 is received [the license request transmitted from the client 1]after performing license issue processing mentioned laterit transmits the license corresponding to license ID contained in a license request to the client 1. The client 1 is saved in the secure state by enciphering the received license at the storage parts store 28if the license transmitted from the license server 4 is received.

[0086]The license with a user needed as mentioned above can be searched and acquired.
[0087]Nextlicense acquisition processing when the user knows license ID of the license needed is shown in drawing 11.
[0088]When a user operates the input part 26inputs license ID and specifies license ID of a license neededCPU21After controlling the communications department 29 and forming a session by mutual recognitionsuch as SSLthe license request containing license ID of a license and terminal ID which were chosen as the contents server 3 via the Internet 2the user ID for fee collectionand a password is encipheredand it transmits. If the license server 4 is received [the license request transmitted from the client 1]after performing license issue processing mentioned laterit transmits the license corresponding to license ID contained in a license request to the client 1. If the license transmitted from the license server 4 is receivedthe client 1 carries out encryption etc. and saves the received license in the secure state at the storage parts store 28.
[0089]License ID can be known from the advertisement of a license etc. in which the user is indicated for the magazine etc. as mentioned aboveand the license for which it asks by specifying the license ID can be acquired.
[0090]The link information of URL of the license server which contains license ID in an HTML filean E-mailetc. of a website is indicatedand it may be made to start license acquisition processing by a user clicking this and choosing it.
[0091]with reference to the flow chart of drawing 12it comes out and the details of drawing 9 - the license issue processing in drawing 11 are explained. The composition of the client 1 of drawing 2 is quoted also as composition of the license server 4 also in this case.
[0092]In Step S102CPU21 incorporates first license IDterminal IDthe user IDand the password which are contained in a license request.
[0093]And CPU21 of the license server 4 accesses the fee collection server 5 from the communications department 29and requires the crediting process of the user corresponding to user ID and a password. If the demand of a crediting process is received from the license server 4 via the Internet 2the fee collection server 5The payment history of the past of the user corresponding to the user ID and passwordetc. are investigatedWhen the credit result which permits grant of a license when it investigates whether there is any track record of the nonpayment of the remuneration of the user's license in the past and there is no such track record is transmitted and there are a track record of nonpaymentetc.the credit result of the disapproval of license granting is transmitted.
[0094]In Step S104CPU21 of the license server 4When it judges whether the credit result from the fee collection server 5 is a credit result which permits giving a license and grant of the license is permittedIt progresses to Step S105the license corresponding to license ID is taken out from a databaseterminal ID is inserted in the

field of the use rule of a licenseand an electronic signature is generated and added with the secret key of the license server 4.
[0095]And it progresses to Step S107 and CPU21 of the license server 4 makes the license to which the terminal ID and electronic signature were added transmit to the client 1 via the Internet 2 from the communications department 29.
[0096]CPU21 of the license server 4 makes the storage parts store 28 memorize the license which is processing of Step S107 and transmitted now in Step S108 corresponding to the user ID and the password which were incorporated by processing of Step S102. In Step S109CPU21 performs accounting. SpecificallyCPU21 requires the accounting to the user corresponding to the user ID and password of the fee collection server 5 from the communications department 29. The fee collection server 5 performs accounting to that user based on the demand of this fee collection. It can be licensedeven if that user demands grant of a license henceforth when that user does not make payment to this accounting as mentioned above.
[0097]That issince the credit result which makes grant of a license disapproval from the fee collection server 5 is transmitted in this caseit progresses to Step S110 from Step S104and CPU21 performs error handling. CPU21 of the license server 4 outputs the message of the purport that a license cannot be givento the client 1 which controlled the communications department 29 and has accessed itandspecificallyterminates processing.
[0098]In this casesince that client 1 cannot be licensed as mentioned abovethose contents can be used.
[0099]Nextthe processing which acquires the contents data of contents with an available license using drawing 13 is explained.
[0100]If a user operates the input part 26 and chooses a licenseCPU will control the communications department 29 and will transmit the contents list demand containing license ID of the license chosen as the contents server 3 via the Internet 2. The license server 4 will take out license ID contained in a contents list demandif a contents list demand is received. The license server 4 extracts available contents from a license database according to an applicable license by using license ID as a key. Thena license server transmits a contents list including contents informationsuch as URL for downloading the content ID of each extracted contentsand contents and a contents namean artist nameand a genreto the client 1.
[0101]If the client 1 controls an outputting part and a contents list is receivedit will display the contents information of each contents contained in a contents list. If the contents to download are chosen with reference to the contents information as which the user was displayedthe client 1 will transmit a contents request to a contents server at the contents server 3 according to URL of contents. A contents server will transmit contents with the content ID contained in a contents request to the client 1if a contents request is received. The client 1 makes the storage parts store 28

memorize the contents which receivedwhen contents are received from the contents server 3.
[0102]You can discover the contents from which a user becomes available according to a license as mentioned aboveand a client can make it download from the contents server 3.
[0103]Drawing 14 expresses the constitution method of the key at the time of adopting broadcasting yne KURIPUSHON (Broadcast Encryption) as the managing system of a key. As shown in drawing 14a key is made into a hierarchy tree structure and leaf (leaf) of the bottom corresponds to each device. In the case of the example of drawing 14the key corresponding to 16 devices from the number 0 to the number 15 is generated.
[0104]Each key is specified corresponding to each node shown by a figure Nakamaru seal. In the keys K00 thru/or K11in this examplethe key K000 thru/or the key K111 correspond [corresponding to the root node of the highest rung / the key KR / the key K0 and K1] corresponding to the 4th node corresponding to the 3rd step of noderespectively corresponding to the 2nd node. And the keys K0000 thru/or K1111 support the leaf (device node) as a node of the bottomrespectively.
[0105]Since it is considered as the layered structurethe key of the higher rank of the key K0010 and the key 0011 is set to K001and the key of the higher rank of the key K000 and the key K001 is set to K00for example. Like the followingthe key of the higher rank of the key K00 and the key K01 is set to K0and the key of the higher rank of the key K0 and the key K1 is set to KR.
[0106]The key used in order to use contents comprises a key corresponding to each node of one path from the device node (leaf) of the bottom to the root node of the highest rung. For examplethe key using the contents of the number 3 comprises each key of the path containing the key K0011K001K00K0and KR.
[0107]In the system of this inventionas shown in drawing 15the hierarchy tree structure keying system which comprises a key corresponding to 8x24x32 steps of nodes is usedfor example. In this keying systema category corresponds to the key corresponding to each node from a root node to eight steps of a low rank. The category in here means categoriessuch as a category of the apparatus which uses semiconductor memorysuch as a memory stickfor exampleand a category of apparatus which receives digital broadcasting.
[0108]In the example of drawing 15the system of this invention corresponds from a root node to one of the 8th step of nodes. By the key corresponding to 24 steps of a younger hierarchy's nodesa license corresponds further from this node. Therebyabout 16 mega (=224= about 1600000) license can be specified. 32 steps of lower hierarchies can prescribe about 4 giga (=232= about 4 billions) of user. The key corresponding to 32 steps of nodes of the bottom constitutes DNK (Device Node Key).
[0109]Each contents correspond to one of the paths which comprise each node of 64

(=8+24+32) stages. That isthe key corresponding to the node which constitutes the assigned path is used for encryption of each contents. It is enciphered using the key of the hierarchy of the latest low rankand the key of the hierarchy of a higher rank is arranged in EKB of drawing 5. DNK of the bottom is not arranged in EKBbut is described by the service information acquired when a client registers with a license serverand as shown in drawing 16it is given to a user's client 1.
[0110]Using DNK described by service informationusing the key which decoded the key of the hierarchy of the latest higher rank described in EKB distributed with contents dataand decoded and obtained itfurthermore the client 1 is described in EKBit decodes the key of the hierarchy on it. By performing the above processing one by onethe client 1 can obtain all the keys belonging to the path of the contents.
[0111]The client 1 can decode the contents key KR (KC) enciphered by KR using KR obtained after performing decoding processing of EKB [more than]and can obtain the contents key KC.
[0112]The key in this invention can also be constituted from keys other than the keying system using broadcasting yne KURIPUSHON as shown in drawing 14 and drawing 15.
[0113]The client to which this invention is applied can be used as PDA (Personal Digital Assistants)a portable telephonea game terminal machineetc. in addition to what is called a personal computer.
[0114]The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings by softwareOr it is installed in the personal computer etc. which can perform various kinds of functionsfor exampleare general-purposeetc. from a network or a recording medium by installing various kinds of programs.
[0115]. As shown in drawing 2this recording medium is distributed apart from a device main frame in order to provide a user with a program. The magnetic disk 41 (a floppy disk is included) with which the program is recordedthe optical disc 42 (CD-ROM (Compact Disk-Read OnlyMemory).) . DVD (Digital Versatile Disk) is included. It is not only constituted by the package media which consist of the magneto-optical disc 43 (MD (Mini-Disk) is included) or the semiconductor memory 44butIt comprises ROM22 with which a user is provided in the state where it was beforehand included in the device main frame and on which the program is recordeda hard disk contained in the storage parts store 28etc.
[0116]In this Descriptioneven if the processing serially performed in accordance with an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed seriallyit also includes a parallel target or the processing performed individually.
[0117]In this Descriptiona system expresses the whole device constituted by two or more devices.
[0118]

[Effect of the Invention]According to the information processor of this invention and a methoda program storing mediumand the programlike the above. The attribution information of the enciphered data and contents is formatted into a predetermined formatmaking it output -- a license -- an attribute condition -- ****** -- it becomes possible to publish a license flexiblycontrolling that data is used unjustlysince it enabled it to decode the data enciphered when it was made like and the attribution information of contents fulfilled the attribute condition of a license.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the contents providing system which applied this invention.
[Drawing 2]It is a block diagram showing the composition of the client of drawing 1.
[Drawing 3]It is a flow chart explaining the download processing of the contents of the client of drawing 1.
[Drawing 4]It is a flow chart explaining contents offer processing of the contents server of drawing 1.
[Drawing 5]It is a figure showing the example of a data format.
[Drawing 6]It is a figure explaining the kind of attribute item.
[Drawing 7]It is a figure showing the composition of a license.
[Drawing 8]It is a flow chart explaining regeneration of a client.
[Drawing 9]It is a flow chart explaining license acquisition processing.
[Drawing 10]It is a flow chart explaining license acquisition processing.
[Drawing 11]It is a flow chart explaining license acquisition processing.
[Drawing 12]It is a flow chart explaining the details of license acquisition processing.
[Drawing 13]It is a flow chart explaining the processing which acquires contents data.
[Drawing 14]It is a figure explaining the composition of a key.
[Drawing 15]It is a figure explaining the composition of a keyand the relation of a license.
[Drawing 16]It is a figure explaining license granting processing of a license server.
[Description of Notations]
1-11-2 [A timer21CPUand 24 / An encryption decoding part25 codec partsand 26 / An input part27 outputting partsand 28 / A storage parts store and 29 / Communications department] A clientthe 2 Internetand 3 A contents server and 4 A license server5 fee-collection serverand 20